Finite LTL Synthesis with Environment Assumptions and Quality Measures
Alberto Camacho, Meghyn Bienvenu, Sheila Mcilraith

To cite this version:

HAL Id: lirmm-01892548
https://hal-lirmm.ccsd.cnrs.fr/lirmm-01892548
Submitted on 10 Oct 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Finite LTL Synthesis with Environment Assumptions and Quality Measures

Alberto Camacho  
Department of Computer Science  
University of Toronto, Canada  
acamacho@cs.toronto.edu

Meghyn Bienvenu  
CNRS, Univ. Montpellier, Inria  
Montpellier, France  
meghyn@lirmm.fr

Sheila A. McIlraith  
Department of Computer Science  
University of Toronto, Canada  
sheila@cs.toronto.edu

Abstract

In this paper, we investigate the problem of synthesizing strategies for linear temporal logic (LTL) specifications that are interpreted over finite traces – a problem that is central to the automated construction of controllers, robot programs, and business processes. We study a natural variant of the finite LTL synthesis problem in which strategy guarantees are predicated on specified environment behavior. We further explore a quantitative extension of LTL that supports specification of quality measures, utilizing it to synthesize high-quality strategies. We propose new notions of optimality and associated algorithms that yield strategies that best satisfy specified quality measures. Our algorithms utilize an automata-game approach, positioning them well for future implementation via existing state-of-the-art techniques.

1 Introduction

The problem of automatically synthesizing digital circuits from logical specifications was first proposed by Church (1957). In 1989, Pnueli and Rosner examined the problem of synthesizing strategies for reactive systems, proposing Linear Temporal Logic (LTL) (Pnueli 1977) as the specification language. In a nutshell, LTL is used to express temporally extended properties of infinite state sequences (called traces), and the aim of LTL synthesis is to produce a winning strategy, i.e., a function that assigns values to the state variables under the control of the system at every time step, in such a way that the induced infinite trace is guaranteed to satisfy the given LTL formula, no matter how the environment sets the remaining state variables.

In 2015, De Giacomo and Vardi introduced the problem of LTL synthesis in which the specification is described in a variant of LTL interpreted over finite traces (De Giacomo and Vardi 2013). Finite interpretations of LTL have long been exploited to specify temporally extended goals and preferences in AI automated planning (e.g., (Bacchus and Kabanza 2000; Baier, Bacchus, and McIlraith 2009)). In contrast to LTL synthesis, which produces programs that run in perpetuity, LTL synthesis is concerned with the generation of terminating programs. Two natural and important application domains are automated synthesis of business processes, including web services; and automated synthesis of robot controllers, in cases where program termination is desired.

Despite recent work on LTL synthesis, there is little written on the nature and form of the LTL specifications and how this relates to the successful and nontrivial realization of strategies for such specifications. LTL synthesis is conceived as a game between the environment and an agent. The logical specification that defines the problem must not only define the desired behavior that execution of the strategy should manifest – what we might loosely think of as the objective of the strategy, but must also define the context, including any assumptions about the environment’s behavior upon which realization of the objective is predicated. As we show in this work, if assumptions about environment behavior are not appropriately taken into account, specifications can either be impossible to realize or can be realized trivially by allowing the agent to violate assumptions upon which guaranteed realization of the objective is predicated.

We further examine the problem of how to construct specifications where the realization of an objective comes with a quality measure, and where strategies provide guarantees with respect to these measures. The addition of quality measures is practically motivated. In some instances we may have an objective that can be realized in a variety of ways of differing quality (e.g., my automated travel assistant may find a myriad of ways for me to get to KR2018 – some more preferable than others!). Similarly, we may have multiple objectives that are mutually unachievable and we may wish to associate a quality measure with their individual realization (e.g., I’d like my home robot to do the laundry, wash dishes, and cook dinner before its battery dies, but dinner is most critical, followed by dishes).

In this paper we explore finite LTL synthesis with environment assumptions and quality guarantees. In doing so, we uncover important observations regarding the form and nature of LTL specifications, how resulting strategies are computed, and the nature of the guarantees we can provide regarding the resulting strategies. In Section 3 we examine the problem of LTL synthesis with environment assumptions, introducing the notion of constrained LTL synthesis in Section 4. In Section 5, we propose algorithms for constrained LTL synthesis, including a reduction to Deterministic Büchi Automata games for the fragment of environment constraints that are conjunctions of safe and co-safe LTL formulae. In Section 6, we examine the problem of augmenting constrained LTL synthesis with quality mea-
tures. We adopt a specification language, LTL[^F], proposed by (Almagor et al. 2017) and define a new notion of optimal strategies. In Section 7, we provide algorithms for computing high-quality strategies for constrained LTL synthesis. Section 8 summarizes our technical contributions. Some proofs are deferred to the appendix. This paper (without the appendix proofs) will appear in the Proceedings of the 16th International Conference on Principles of Knowledge Representation and Reasoning (KR 2018).

2 Preliminaries

We recall the syntax and semantics of linear temporal logic for both infinite and finite traces, as well as the basics of finite state automata and the link between LTL and automata.

2.1 Linear Temporal Logic (LTL)

Given a set Ψ of propositional variables, LTL formulæ are defined as follows:

\[ ϕ ::= T | \bot | p | ¬ϕ | ϕ_1 \land ϕ_2 | ϕ_1 \lor ϕ_2 | \square ϕ | ϕ_1 U ϕ_2 | ϕ_1 R ϕ_2 \]

where \( p \in Ψ \). Here, \( \land \), \( \lor \), and \( \bot \) are the usual Boolean connectives, and \( \square \) (next), \( U \) (until), and \( R \) (release) are temporal operators. The formula \( ϕ \) states that \( ϕ \) must hold in the next timepoint, \( ϕ_1 U ϕ_2 \) stipulates that \( ϕ_1 \) must hold until \( ϕ_2 \) becomes true, and \( ϕ_1 R ϕ_2 \) expresses that \( ϕ_2 \) remain true until and including the point in which \( ϕ_1 \) is made true (or forever if \( ϕ_2 \) never becomes true). For concision, we do not include logical implication \((\rightarrow)\), eventually \((\lozenge, \text{‘sometime in the future’})\) and always \((\Box, \text{‘at every point in the future’})\) in the core syntax, but instead view them as abbreviations:

\[ α \rightarrow β := \neg α \lor β, \quad \square α := \top U α \quad \text{and} \quad \Box α := \bot R α. \]

LTL formulæ are traditionally interpreted over infinite traces \( π \), i.e., infinite words over the alphabet \( 2^Ψ \). Intuitively, an infinite trace \( π \) describes an infinite sequence of (time)steps, with the \( i \)-th symbol in \( π \), written \( π(i) \), specifying the propositional symbols that hold at step \( i \). We use \( π \subseteq π' \) to indicate that \( π \) is a prefix of \( π' \). We define what it means for an infinite trace \( π \) to satisfy an LTL formula \( ϕ \) at step \( i \), denoted \( π \models_i ϕ \):

- \( π \models_i T \iff \bot \)
- \( π \models_i p \iff p \in π(i) \), for each \( p \in Ψ \)
- \( π \models_i \neg ϕ \iff \neg π \models_i ϕ \)
- \( π \models_i ϕ_1 \land ϕ_2 \iff \pi \models_i ϕ_1 \quad \text{and} \quad \pi \models_i ϕ_2 \)
- \( π \models_i ϕ_1 \lor ϕ_2 \iff \pi \models_i ϕ_1 \quad \text{or} \quad \pi \models_i ϕ_2 \)
- \( π \models_i \square ϕ \iff \pi \models_{i+1} ϕ \)
- \( π \models_i ϕ_1 U ϕ_2 \iff \exists j \geq i \text{ such that } \pi \models_j ϕ_2 \quad \text{and} \quad \forall i < k \text{ such that } \pi \models_k ϕ_1 \)
- \( π \models_i ϕ_1 R ϕ_2 \iff \forall j \geq i \text{ either } \pi \models_j ϕ_2 \text{ or } \exists i \leq k < j \text{ such that } \pi \models_k ϕ_1 \).

A formula \( ϕ \) is satisfied in \( π \), written \( π \models ϕ \), if \( π \models_1 ϕ \). Two formulæ \( ϕ \) and \( ψ \) are equivalent if \( π \models ϕ \iff π \models ψ \) for all traces \( π \). Observe that, in addition to the usual Boolean equivalences, we have the following:

\[ ϕ_1 U ϕ_2 \equiv \neg(\square \neg ϕ_1 \land ϕ_2) \quad \text{and} \quad \Box ϕ \equiv \neg ϕ \land ϕ U \top. \]

We consider two well-known syntactic fragments of LTL.

The safe fragment is defined as follows (Sistla 1994):

\[ ϕ ::= T | \top | p | \neg p | ϕ_1 \land ϕ_2 | \square ϕ | ϕ_1 U ϕ_2 | ϕ_1 R ϕ_2 \]

The complementary co-safe fragment is similarly defined, using \( U \) in place of \( R \). It is known that if \( ϕ \) is a safe formula and \( π \not\models ϕ \), then there is a finite bad prefix \( π_b \subseteq π \) such that \( π' \not\models ϕ \) for every infinite trace \( π' \) with \( π_b \not\subseteq π' \). Similarly, if \( ϕ \) is a co-safe formula and \( π \models ϕ \), then there exists a finite good prefix \( π_g \subseteq π \) such that \( π' \models ϕ \) for every infinite trace \( π' \) with \( π_g \not\subseteq π' \). This means that violation of safe formulæ and satisfaction of co-safe formulæ can be shown by exhibiting a suitable finite prefix (Kupferman and Vardi 2001).

In this paper, our main focus will be on a more recently studied finite version of LTL, denoted LTL[π] (De Giacomo and Vardi 2013), in which formulæ are interpreted over finite traces (finite words over \( 2^Ψ \)). We will reuse the notation \( π(ι) \) (i-th symbol) and introduce the notation \( |π| \) for the length of \( π \). LTL[π] has precisely the same syntax as LTL and the same semantics for the propositional constructs, but it differs in its interpretation of the temporal operators:

- \( π(ι) \models \Box ϕ \iff |π| > i \) and \( π|_{ι+1} ϕ \)
- \( π(ι) \models ϕ_1 U ϕ_2 \iff \text{there exists } i \leq j \leq |π| \text{ such that } π|_j ϕ_2 \text{ and } π|_k ϕ_1 \text{, for each } i < k < j \)
- \( π(ι) \models ϕ_1 R ϕ_2 \iff \text{for all } i \leq j \leq |π| \text{ either } π|_j ϕ_2 \text{ or there exists } i < k < j \text{ such that } π|_k ϕ_1 \)

We introduce the weak next operator \( (\diamond) \) as an abbreviation:

\[ ϕ \models (\diamond ϕ) \iff ϕ \models \Box ϕ \land \neg ϕ \]

Thus, \( ϕ(ι) \models \diamond ϕ \) if \( ϕ(ι) \models \Box ϕ \) in the next time step or we have reached the end of the trace. Over finite traces, \( \neg ϕ \equiv \Box \neg ϕ \), but we do have \( \neg ϕ \equiv \neg ϕ \).

As before, we say that \( ϕ \) is satisfied in \( π \), written \( π \models ϕ \), if \( π \models_1 ϕ \). Note that we can unambiguously use the same notation for LTL and LTL[π] so long as we specify whether the considered trace is finite or infinite.

2.2 Finite State Automata

We recall that a non-deterministic finite-state automaton (NFA) is a tuple \( A = (Σ, Q, q_0, F) \), where \( Σ \) is a finite alphabet of input symbols, \( Q \) is a finite set of states, \( Q_0 \subseteq Q \) is a set of initial states, \( F \subseteq Q \) is a set of accepting states, and \( δ : Σ \times Q \rightarrow 2^Q \) is the transition function. NFAs are evaluated on finite words, i.e. elements of \( Σ^* \). A run of \( A \) on a word \( w = b_1 \cdots b_n \) is a sequence \( q_0 \cdots q_n \) of states, such that \( q_0 \in Q_0 \), and \( q_{i+1} \in δ(q_i, b_{i+1}) \) for all \( 0 \leq i < n \). A run \( q_0 \cdots q_n \) is accepting if \( q_n \in F \), and \( A \) accepts \( w \) if some run of \( A \) on \( w \) is accepting. The language of an automaton \( A \), denoted \( L(A) \), is the set of words accepted by \( A \).

Deterministic finite state automata (DFAs) are NFAs in which \( |Q_0| = 1 \) and \( |δ(q, Σ)| = 1 \) for all \( (q, σ) \in Σ \times Q \). When \( A \) is a DFA, we define \( δ(Q) : Q \times Σ \rightarrow 2^Q \) and \( q^* = δ(q, θ) \) in place of \( q' = δ(q, σ) \) and when \( Q_0 = \{q_0\} \), we will simply write \( q_0 \) (without the set notation). For every NFA \( A \), there exists a DFA that accepts the same language as \( A \) and whose size is at most single exponential in the size of \( A \). The powerset construction is a well-known technique to determinize NFAs (Rabin and Scott 1959).

Non-deterministic Büchi automata (NBA) are defined like NFAs but evaluated on infinite words, that is, elements of \( Σ^* \). A run of \( A \) on an infinite word \( w = b_1b_2 \cdots \) is a sequence \( ρ = q_0q_1q_2 \cdots \) of states, such that \( q_0 \in Q_0 \), and \( q_{i+1} \in δ(q_i, b_{i+1}) \) for every \( i \geq 0 \). A run \( ρ \) is accepting if \( \text{inf}(ρ) \cap F \neq \emptyset \), where \( \text{inf}(ρ) \) is the set of states that appear infinitely often in \( ρ \). We say that an NBA \( A \) accepts \( w \) if some run of \( A \) on \( w \) is accepting. Analogous definitions apply to deterministic Büchi automata (DBAs).
We will also consider deterministic finite-state transducers (also called Mealy machines, later abbreviated to ‘transducers’), given by tuples $T = \langle \Sigma, \Omega, Q, \delta, \omega, q_0 \rangle$, where $\Sigma$ and $\Omega$ are respectively the input and output alphabets, $Q$ is the set of states, $\delta : Q \times \Sigma \rightarrow Q$ is the transition function, $\omega : Q \times \Sigma \rightarrow \Omega$ is the output function, and $q_0$ the initial state. The run of $T$ on $w = \theta_1 \theta_2 \ldots \in \Sigma^\omega$ is an infinite sequence of states $q_0 \theta_1 \delta(\theta_1, q_0) \delta(\theta_2, q_0) \delta(\theta_3, q_0) \ldots$ for each $i \geq 0$, and the output sequence of $T$ on $w$ is $\omega(q_0) \theta_1 \omega(\delta(\theta_1, q_0)) \theta_2 \omega(\delta(\theta_2, q_0)) \theta_3 \omega(\delta(\theta_3, q_0)) \ldots$.

Given an LTL formula $\varphi$, one can construct an NFA that accepts precisely those finite traces $\pi$ with $\pi \models \varphi$ (e.g. (De Giacomo and Vardi 2015)). For every safe formula $\varphi$ (resp. co-safe formula $\neg \varphi$), one can construct an NFA that accepts all bad prefixes of $\varphi$ (resp. good prefixes of $\varphi$) (Kupferman and Vardi 2001). In these constructions, the NFAs are worst case single exponential in the size of the formula. By determining these NFAs, we can obtain DFAs of double-exponential size that recognize the same languages.

### 3 LTL and LTL₁ Synthesis

To set the stage for our work, we recall the definition of LTL synthesis in the infinite and finite trace settings and the relationship between planning and synthesis.

#### 3.1 LTL Synthesis

An LTL specification is a tuple $(X, Y, \varphi)$ where $\varphi$ is an LTL formula over uncontrollable variables $X$ and controllable variables $Y$. A strategy is a function $\sigma : (2^X)^\omega \rightarrow 2^Y$. The infinite trace induced by $\sigma$ is $\pi[\sigma, X] = \{X[i]_{i \geq 1} \in (2^X)^\omega \text{ and } \pi \models \varphi \mid X \in (2^X)^\omega \}$.

The set of all infinite traces induced by $\sigma$ is denoted $\text{traces}(\sigma)$. The realizability problem $(X, Y, \varphi)$ consists in determining whether there exists a winning strategy, i.e., a strategy $\sigma$ such that $\sigma \models \varphi$ for every $\pi \in \text{traces}(\sigma)$. The synthesis problem is to compute such a winning strategy when one exists.

LTL synthesis can be viewed as a 2-player game between the environment $(X)$ and the agent $(Y)$. In each turn, the environment makes a move by selecting $X_i \subseteq X$, and the agent replies by selecting $Y_i \subseteq Y$. The aim is to find a strategy $\sigma$ for the agent that guarantees the resulting trace satisfies $\varphi$.

#### 3.2 Finite LTL Synthesis

We now recall LTL₁ realizability and synthesis, an LTL specification is interpreted over finite traces. An LTL₁ specification is a tuple $(X, Y, \varphi)$, where $\varphi$ is an LTL₁ formula over uncontrollable variables $X$ and controllable variables $Y$. A strategy for an LTL₁ specification $\sigma : (2^X)^n \rightarrow 2^Y$ is a function such that for each finite sequence $X = \{X[i]_{i \leq n} \in (2^X)^n \}$ of subsets of $X$, there is exactly one integer $n > 0$ with $\pi_n[\sigma[X], X]$, the induced infinite trace $\pi[\sigma, X]$ is defined as before, and the finite trace induced by $X$ and $\sigma$ is $\pi[\sigma[X], X] = (X[0] \cup \sigma(X[1])) \ldots (X[n-X] \cup \sigma(X[1] \ldots X[n-X]))$ but with $\pi_n$ removed from $\sigma(X[1] \ldots X[n-X])$. The set of all finite traces induced by $\sigma$ is denoted $\text{traces}^*(\sigma)$. A finite trace $\pi$ is compatible with $\sigma$ if $\pi \in \text{traces}^*(\sigma)$. for some $\pi' \in \text{traces}^*(\sigma)$, with $\text{ptraces}(\sigma)$ (‘$\pi'$ for ‘partial’) the set of all such traces. We call $\sigma$ a winning strategy for an LTL₁ specification $(X, Y, \varphi)$ if $\pi \models \varphi$ for every $\pi \in \text{traces}(\sigma)$. The realizability and synthesis problems for LTL₁ are then defined in the same way as for LTL.

#### 3.3 Planning as LTL₁ Synthesis

It has been observed that different forms of automated planning can be recast as LTL₁ synthesis (see e.g. (De Giacomo and Vardi 2015; D’Ippolito, Rodríguez, and Sardiña 2018; Camacho et al. 2018b)). We recall that planning problems are specified in terms of a set of fluents (i.e., atomic facts whose value may change over time), a set of actions which can change the state of the world, an action theory whose axioms give the preconditions and effects of the actions (i.e., which fluents must hold for an action to be executable, and how do the fluents change as a result of performing an action), a description of the initial state, and a goal. In classical planning, actions are deterministic (i.e. there is a unique state resulting from performing an action in a given state), and the aim is to produce a sequence of actions leading from the initial state to a goal state. In fully observable non-deterministic (FOND) planning, actions have non-deterministic effects, meaning that there may be multiple possible states that result from performing a given action in a given state (with the effect axioms determining which states are possible results). Strong solutions are policies (i.e., functions that map states into actions) that guarantee eventual achievement of the goal.

We briefly describe how FOND planning can be reduced to LTL₁ synthesis, but as the reduction crucially relies on the use of environment assumptions. We will use the set $F$ of fluents as the uncontrollable variables, and the set of actions $A$ for the controllable variables. The high-level structure of the LTL₁ specification formula is: $\Phi = (\Psi_{\text{init}} \land \Psi_{\text{eff}}) \rightarrow (\Psi_{\text{pre}} \land \Psi_{\text{goal}})$. Intuitively, $\Phi$ states that under the assumption that the environment sets the fluents in accordance with the initial state and effect axioms (captured by $\Psi_{\text{init}}$ and $\Psi_{\text{eff}}$), the agent can choose a single action per turn ($\Psi_{\text{one}}$) in such a way that the preconditions are obeyed ($\Psi_{\text{pre}}$) and the goal is achieved ($\Psi_{\text{goal}}$). We set $\Psi_{\text{goal}} = 0(\gamma \land \neg G\top)$.
where \( \gamma \) is a propositional formula over \( F \) describing goal states. The formula \( \Psi_{\text{one}} = \Omega \psi_{\text{one}} \) with \( \psi_{\text{one}} = (\Box T \leftrightarrow \bigwedge_{a \in A} (a \rightarrow \rho_a)) \) and \( \bigwedge_{a \in A} (a \rightarrow \rho_a) \) enforces that a single action is performed at each step. The formula \( \Psi_{\text{pre}} \) can be defined as \( \bigwedge_{a \in A} (a \rightarrow \rho_a) \), where \( \rho_a \) is a propositional formula over \( F \), typically a conjunction of literals, that gives the preconditions of \( a \). The formula \( \Psi_{\text{init}} \) will simply be the conjunction of literals over \( F \) corresponding to the initial state. Finally, \( \Psi_{\text{eff}} \) will be a conjunction of formulas of the form

\[
\Box ((\kappa \land a \land \rho_a \land \psi_{\text{one}}) \rightarrow \Box \beta)
\]

where \( a \in A \) and \( \kappa \) and \( \beta \) are propositional formulas over \( F \).

### 3.4 Illustrative Example

We now give a concrete example of an LTL\(_f\) synthesis problem, which illustrates the importance of environment assumptions. Consider synthesizing a high-level control strategy for your Roomba-style robot vacuum cleaner. You want the robot to clean the living room (LR) and bedroom (BR) when they are dirty, but you don’t want it to vacuum a room while your cat is there (the robot scares her). We now discuss why it is important to include \( \rho_a \land \psi_{\text{one}} \).

Taking inspiration from the encoding of planning, we will use \( \{\text{clean}(z), \text{catIn}(z) \mid z \in \{LR, BR\}\} \) (the fluents\(^2\) in our scenario) as the set of uncontrollable variables, and take the robot’s actions \( \{\text{vac}(BR), \text{vac}(LR)\} \) as the controllable variables. As was the case for planning, it is natural to conceive of the specification as having the form of an implication \( \Psi_{\text{env}} \rightarrow \Psi_{\text{robot}} \), with \( \Psi_{\text{env}} \) describing the rules governing the environment’s behavior and \( \Psi_{\text{robot}} \) the desired behavior of the robot. We define \( \Psi_{\text{env}} \) as the conjunction of:

- for \( z \in \{LR, BR\} \), the formula \( \Box (\text{vac}(z) \rightarrow \rho_{\text{vac}}(z)) \) with \( \rho_{\text{vac}} = \neg\text{clean}(z) \land \neg\text{catIn}(z) \) (the precondition of \( \text{vac}(z) \) (we can only vacuum dirty cat-free rooms));
- \( \bigcirc (\neg\text{vac}(LR) \lor \neg\text{vac}(BR)) \) (we cannot vacuum in two places at once);
- \( \Box (\text{clean}(LR) \land \text{clean}(BR)) \) (our goal: both rooms clean).

We let \( \rho_{\text{vac}} = \text{vac}(z) \land \rho_{\text{vac}} \land \neg\text{catIn}(z) \) (z the other room) encode a correct execution of \( \text{vac}(z) \), and let \( \Psi_{\text{init}} \) be a conjunction of the following:

- for \( z \in \{LR, BR\} \), the formula \( \Box (\text{clean}(z) \lor \varphi_{\text{vac}}(z) \rightarrow \Box \text{clean}(z)) \) (if room \( z \) is currently clean, or if the robot correctly performs action \( \text{vac}(z) \), then room \( z \) is clean in the next state\(^3\));
- for \( z \in \{LR, BR\} \), the formula \( \Box (\neg\text{clean}(z) \land \neg\text{catIn}(z) \rightarrow \Box \text{clean}(z)) \) (a room can only become clean if it is vacuumin); \( \bigcirc (\neg\text{catIn}(LR) \land \neg\text{catIn}(BR)) \) and \( \bigcirc (\text{catIn}(LR) \land \text{catIn}(BR)) \) (the cat is in exactly one of the rooms).

As the reader may have noticed, while the assumptions in \( \Psi_{\text{env}} \) are necessary, they are not sufficient to ensure realizability, as the cat may stay forever in a dirty room.

---

\(^2\)We use notation reminiscent of first-order logic to enhance readability, but the variables (e.g. \( \text{clean}(LR) \)) are propositional.

\(^3\)For simplicity, we assume once a room is clean, it stays clean.

we further assume that the cat eventually leaves each of the rooms (\( \varphi_{\text{leaves}} = \neg\text{catIn}(BR) \land \neg\text{catIn}(LR) \)), there is an obvious solution: vacuum a cat-free room, and then simply wait until the other room is cat-free and then vacuum it. However, rather unexpectedly, adding \( \varphi_{\text{leaves}} \) to \( \Psi_{\text{env}} \) makes the specification \( \Psi_{\text{env}} \rightarrow \Psi_{\text{robot}} \) realizable in a trivial and unintended way: by ending execution in the first move, \( \neg\Psi_{\text{env}} \) trivially holds in the resulting length-1 trace \( \pi \). Indeed, there are three possibilities: (i) \( \pi \models \text{catIn}(BR) \) (so \( \pi \models \neg\text{catIn}(LR) \)), (ii) \( \pi \models \text{catIn}(LR) \) (so \( \pi \models \neg\text{catIn}(BR) \)), or (iii) \( \pi \models \neg\text{catIn}(LR) \land \neg\text{catIn}(BR) \) (so \( \pi \models (\bigcirc (\text{catIn}(LR) \lor \text{catIn}(BR)) \)). Clearly, this length-1 strategy is not the strategy that we wanted to synthesize. In Section 4, we propose a new framework for handling environment assumptions which avoids the generation of such trivial strategies and makes it possible to find the desired strategies.

### 4 Constrained LTL\(_f\) Synthesis

To the aim of properly handling environment assumptions, we introduce a generalization of LTL\(_f\) synthesis, in which the assumptions are separated from the rest of the specification formula and given a different interpretation. Essentially, the idea is that the environment is allowed to satisfy the assumption over the whole infinite trace, rather than on the finite prefix chosen by the agent. This can be accomplished using LTL semantics for the environment assumption, but keeping LTL\(_f\) semantics for the formula describing the objective.

Formally, a constrained LTL\(_f\) specification is a tuple \((X, \gamma, \alpha, \varphi)\), where \( X \) and \( \gamma \) are the uncontrollable and controllable variables, \( \varphi \) is an LTL formula over \( X \cup \gamma \), and \( \alpha \) is an LTL formula over \( X \cup \gamma \). Here \( \varphi \) describes the desired agent behavior when the environment behaves so as to satisfy \( \alpha \). We will henceforth call \( \varphi \) the objective, and will refer to \( \alpha \) as the (environment) assumption or constraint (as it acts to constrain the allowed environment behaviors).

A strategy for \((X, \gamma, \alpha, \varphi)\) is a function \( \sigma : (2^X)^* \rightarrow 2^{(\gamma \cup \{\text{end}\})} \) such that for each infinite sequence \( X = [X_i]_{i \geq 1} \in (2^X)^* \) of subsets of \( X \), there is at most one integer \( n_x \geq 1 \) with \( \text{end} \in \sigma(X_1 \cdots X_{n_x}) \). If none exists, we write \( n_x = \infty \). To account for traces that do not contain \text{end}, we redefine traces\(^4\) as follows: \( [n_1 \sigma \mid \tau \in (2^X)^*] \) and \( n_x = \infty \). A strategy \( \sigma \) is an \( \alpha \)-strategy if for every \( \tau \in (2^X)^* \), either \( n_x < \infty \) or \( \sigma[X] \not\models \alpha \), i.e. \( \sigma \) terminates on every trace that satisfies \( \alpha \). A winning strategy (w.r.t. \((X, \gamma, \alpha, \varphi)\)) is an \( \alpha \)-strategy such that \( \pi \models \varphi \) for every \( \pi \) in traces\(^4\) \( (\sigma) \). In other words, winning strategies are those that guarantee the satisfaction of the objective \( \varphi \) under the assumption that the environment behaves in a way that constraint \( \alpha \) is satisfied. The realizability and synthesis problems for constrained LTL\(_f\) specifications are defined as before, using this notion of winning strategy.

Because the constraints are interpreted using infinite LTL semantics, we are now able to correctly handle liveliness constraints (\( \Box \varphi \)) and fairness constraints as studied in LTL synthesis (\( \Box \varphi \)) and FOND planning (\( \Box \varphi_1 \rightarrow \Box \varphi_2 \)) (D’Ippolito, Rodríguez, and Sardinha 2018).

#### Example 1

Returning to our earlier example, consider the constrained synthesis problem with assumption \( \Psi_{\text{env}} \) (which
includes ϕ_{\text{leaves}}) and objective ψ_{\text{safe}}. The obvious strategy (vacuum dirty rooms as soon as they are cat-free) gives rise to a winning strategy, in which we output end if we manage to clean both rooms, and otherwise, produce an infinite trace without end in which ψ_{\text{safe}} is not true. Trivial strategies that terminate immediately will not be winning strategies, as there will be infinite traces that satisfy the constraint but where the length-1 finite trace falsifies the objective.

We remark that if we are not careful about how we write the constraint α, we may unintentionally allow the agent to block the environment from fulfilling α.

**Remark 1.** Suppose that instead of using Equation 1 to encode the effects of actions, we employ the simpler □((κ ∧ α) → (ϕ ∨ y)). While intuitive, this alternative formulation does not properly encode FOND planning, as the specification may be realized in an unintended way: by performing multiple actions with conflicting effects, or a single action whose precondition is not satisfied, the agent can force the environment to satisfy a contradictory set of formulae β in the next state, causing the assumption to be violated.

Chatterjee, Henzinger, and Jobstmann (2008) discuss this phenomenon in the context of LTL synthesis, and suggest that a reasonable environment constraint is one which is realizable for the environment. We note that the constraints we considered in Section 3 all satisfy this property.

**Correspondence with Finite LTL Synthesis** We begin by observing that (plain) LTL synthesis is a special case of constrained LTL synthesis in which one uses the trivial constraint □ for the environment assumption:

**Theorem 1.** Every winning strategy σ for the LTL specification (X, Y, α) is a winning strategy for the constrained LTL specification (X, Y, □, α), and vice-versa. In particular, (X, Y, α) is realizable iff (X, Y, □, α) is realizable.

A natural question is whether a reduction in the other direction exists. Indeed, it is well-known that in the infinite setting, assume-guarantee LTL synthesis with an assumption α and objective ϕ corresponds to classical LTL synthesis w.r.t. α → ϕ (that is, the two synthesis problems have precisely the same winning strategies). The following negative result shows that a simple reduction via implication does not work in the finite trace setting:

**Theorem 2.** There exists an unrealizable constrained LTL specification S = (X, Y, α → ϕ) such that the LTL specifications S\_α = (X, Y, α → ϕ) is realizable.

**Proof.** Consider the constrained LTL specification S = \{⟨x, x′⟩, [y], α, ϕ\} with α = ¬x ∧ 0x and ϕ = 0(x′ ∧ y). We claim that S is unrealizable. Indeed, take any X = X_1X_2... such that x \not∈ X_1, x \in X_2, and x′ \not∈ X_i for all i ≥ 1. Then no matter which strategy σ is used, the infinite trace π[σ, X] will satisfy α, and the induced finite trace π^f[σ, X], if it exists, will falsify ϕ (as x′ never holds).

Next consider S\_α = \{⟨x, [y], α → ϕ⟩, and observe that α → ϕ ≡ x ν (¬(ν x) ν (0(x′ ∧ y). A simple winning strategy exists: output end in the first time step. Indeed, every induced trace has length 1 and hence trivially satisfies x ∨ □. □

With the next theorem, we observe a more fundamental difficulty in reducing constrained LTL synthesis problems to standard LTL synthesis: winning strategies for constrained problems may need an unbounded number of time steps to realize the specification, a phenomenon that does not occur in standard LTL synthesis.

**Theorem 3.** An LTL specification is realizable if it admits a bounded winning strategy, i.e. a strategy for which there exists B > 0 such that every induced finite trace has length at most B. There exist realizable constrained LTL specifications that do not possess any bounded winning strategy.

**Proof.** A straightforward examination of the LTL synthesis algorithm in (De Giacomo and Vardi 2015) shows that when (X, Y, α) is realizable, the produced strategy guarantees achievement of ϕ in a finite number of time steps bounded by the number of states in a DFA for ϕ.

For the second point, consider the constrained LTL specification S = \{⟨x⟩, [y], α, ϕ⟩, Assume for a contradiction that there is a winning strategy σ for S and constant B > 0 such that n_{σ, X} ≤ B for every X ∈ X^\ω. Define X^α = X_1X_2... as follows: X^α_i = ⟨x⟩ if i = B + 1 and X^α_i = Ø otherwise. The induced trace π = π[σ, X^α] has length at most B and hence does not contain x. It follows that π \not∈ ϕ, contradicting our assumption that σ is a winning strategy. □

While the implication-based approach does not work in general, we show that it can be made to work for environment assumptions that belong to the safe fragment:

**Theorem 4.** When α is a safe formula, the constrained LTL specification S = (X, Y, α → ϕ) is realizable if the LTL specification S\_α = (X, Y, α → ϕ) is realizable, where α\_α is obtained from α by replacing every occurrence of x/ϕ by □ϕ.

**Proof.** Sketch. Let σ\_α be a winning strategy for (X, Y, α\_α → ϕ), with α a safe formula. To define a winning strategy σ for (X, Y, α, ϕ), we set σ(X_1...X_n) =

- σ(X_1...X_n) \{end\}, when end \in σ(X_1...X_n) and
  \{X_i \cup σ(X_i) : i \in \rho(X_1...X_n)\} ⊈ α;
- σ(X_1...X_n), otherwise.

For the other direction, given a winning strategy σ for (X, Y, α, ϕ), we define a winning strategy σ\_α for (X, Y, α\_α → ϕ) by setting σ\_α(X_1...X_n) equal to

- σ(X_1...X_n) \{end\}, if \{X_1 \cup σ(X_1) : i < n\} is a bad prefix for α, and end \not∈ σ\_α(X_1...X_n) for k < n;
- σ(X_1...X_n) \{end\}, if end \in σ\_α(X_1...X_n) for some k < n;
- σ\_α(X_1...X_n) = σ(X_1...X_n), otherwise. □

4The algorithm can be easily modified to output end once ϕ has been satisfied to match our definition of strategy.
The following example shows that it is essential in the preceding case to use \( \alpha' \to \varphi \) rather than \( \alpha \to \varphi \):

**Example 2.** If we let \( \alpha = \Box(\neg x \lor q(x)) \) and \( \varphi = \neg x \land y \), then the constrained specification \( \langle X, Y, \alpha, \varphi \rangle \) is not realizable (as the environment can output \( x \) in the first step), but the LTL specification \( \langle X, Y, \alpha \to \varphi \rangle \) is realizable with a strategy that outputs \( (y, \text{end}) \) in the first step. Indeed, if the environment outputs \( x \), then \( \neg \alpha \equiv (x \land \neg q(x)) \) holds in the induced length-1 trace; if we have \( \neg x \) instead, then \( \varphi \) holds.

Note however that the negative result in the general case (Theorem 6) continues to hold if \( \alpha' \to \varphi \) is used instead of \( \alpha \to \varphi \), since the formulas in that proof do not involve \( \Box \).

Another interesting observation is the environment assumptions \( \Psi_{out} \) and \( \Psi_{ef} \) used to encode the initial state and action effects in planning are safe formulas. This explains why these constraints can be properly encoded in LTLf using implication and \( \Box \) rather than \( \varphi \). We note that if we encode planning using constrained LTLf synthesis, then we can use \( \Box \) in the effect axioms, which is arguably more natural.

**Reduction to LTL Synthesis** Every LTLf formula \( \varphi \) over \( P \cup \{\text{alive}\} \) can be polynomially transformed into an LTL formula \( \varphi_{\text{end}} \) over \( P \cup \{\text{alive}\} \) such that \( \pi \models \varphi_{\text{end}} \iff \pi \models \varphi \) for some finite prefix \( \pi \in \pi \) (De Giacomo and Vardi 2013). Intuitively, alive holds for the duration of the (simulated) finite trace. Formally, \( \varphi_{\text{end}} \equiv \tau(\varphi) \land \text{alive} (\equiv \Box(\text{alive}\lor \Box(\text{alive}))) \), where:

\[
\tau(p) = \begin{cases} 
\tau(\neg \varphi) = \neg \tau(\varphi) & \tau(\varphi_1 \land \varphi_2) = \tau(\varphi_1) \land \tau(\varphi_2) \\
\tau(\varphi(\psi)) = \Box(\tau(\varphi) \land \text{alive}) \land \text{alive} \lor \Box(\tau(\varphi)) \land \text{alive} \lor \Box(\tau(\varphi)) \land \text{alive} 
\end{cases}
\]

We extend this transformation as follows:

\[
\psi_{\text{end}} = \Box(\text{end} \iff \text{alive} \lor \Box(\text{alive} \land \text{end})) \land \Box(\text{end} \to \Box(\text{alive} \land \text{end}))
\]

Here \( \psi_{\text{end}} \) forces the agent to trigger variable \text{end} when the end of the trace is simulated and also ensures that \( \text{end} \) occurs at most once. Formula \( \psi_{\text{end}} \) ensures that \( \varphi_{\text{end}} \) is satisfied – i.e., a finite trace that satisfies \( \varphi \) and \( \text{end} \) is simulated – when either the environment assumption \( \alpha \) holds or \( \text{end} \) occurs.

**Theorem 5.** The constrained LTLf specification \( S = \langle X, Y, \alpha, \varphi \rangle \) is realizable iff LTL specification \( S' = \langle X, Y, \alpha, \psi_{\text{end}} \rangle \) is realizable. Moreover, for every winning strategy \( \sigma \) for \( S' \), the strategy \( \sigma' \) defined by \( \sigma'(X_1 \cdots X_n) = \sigma(X_1 \cdots X_n) \land \{\text{alive}\} \) is a winning strategy for \( S \).

### 5 Algorithms for Constrained LTLf Synthesis

LTL and LTLf realizability are both 2EXP-complete (Pnueli and Rosner 1989; De Giacomo and Vardi 2015), and we can show the same holds for constrained LTLf problems. The upper bound exploits the reduction to LTL (Theorem 5), and the lower bound is inherited from (plain) LTLf synthesis, which is a special case of constrained LTLf synthesis (Theorem 1).

**Theorem 6.** Constrained LTLf realizability (resp. synthesis) is 2EXP-complete (resp. in 2EXP).

It follows from Theorem 6 that the reduction to infinite LTL realizability and synthesis yields worst-case optimal algorithms. However, we argue that the reduction to LTL does not provide a practical approach. Indeed, while LTL and LTLf synthesis share the same worst-case complexity, recent experiments have shown that LTLf is much easier to handle in practice (Zhu et al. 2017). Indeed, state-of-the-art approaches to LTLf synthesis rely on translating the LTL formula into a suitable infinite-word automaton, then solving a two-player game on the resulting automaton. The computational bottleneck is the complex transformations of infinite-word automata, for which no efficient implementations exist. Recent approaches to LTLf synthesis also adopt an automata-game approach, but LTLf formulae require only finite-word automata (NFAs and DFAs), which can be manipulated more efficiently.

The preceding considerations motivate us to explore an alternative approach to constrained LTLf synthesis, which involves a reduction to DBA games. Importantly, the DBA can be straightforwardly constructed from DFAs for the constraint and objective formulae, allowing us to sidestep the difficulties of manipulating infinite-word automata.

### 5.1 DBA for Constrained Specifications

For the rest of this section, we assume \( \alpha = \alpha_s \land \alpha_c \), where \( \alpha_s \) is a safe formula and \( \alpha_c \) is a co-safe formula, both defined over \( X \cup Y \). Safe and co-safe formulae are well-known LTL fragments (Kupferman and Vardi 2001) of proven utility. Safe formulae are prevalent in LTL specifications and a key part of the encoding of planning as LTLf synthesis (see Section 3.3); the usefulness of co-safe formula can be seen from our example (Section 3.4) and their adoption in work on robot planning (see e.g. (Lahijanian et al. 2015)).

Our aim is to construct a DBA that accepts infinite traces \( \pi \) over \( X \cup Y \) such that either (i) \( \pi \) contains a single occurrence of \( \text{end} \) which induces a finite prefix \( \pi' \neq \varnothing \) or (ii) \( \pi \) doesn’t contain \( \text{end} \) and \( \pi \models \alpha_s \land \alpha_c \). Such a DBA \( \mathcal{A}_C^{\alpha_s, \alpha_c} \) can be defined by combining three DFAs: \( \mathcal{A}_R \equiv (2^P, Q_s, \delta_s, (q_0), F_s) \) accepts the bad prefixes of \( \alpha_s \); \( \mathcal{A}_C \equiv (2^P, Q_c, \delta_c, (q_0), F_c) \) accepts the good prefixes of \( \alpha_c \); and \( \mathcal{A}_P \equiv (2^P, Q_p, \delta_p, (q_0), F_p) \) accepts models of \( \varphi \). Recall that these DFAs can be built in double-exponential time.

Formally, we let \( \mathcal{A}_C^{\alpha_s, \alpha_c} = (2^{X\cup Y\cup\{\text{end}\}}, Q, \delta, q_0, F) \), where \( Q, q_0, F \) and \( D \) as follows:

- \( Q := (Q_s \cup \{\text{bad}\} \times (Q_c \cup \{\text{good}\} \times Q_p)) \cup \{q_T, q_L\} \)
- \( q_0 := ((q_0), (q_0), (q_0)) \)
- \( F := \{q_s, q_c, q_p\} \cup \{q_T, q_L\} \)

For ‘regular’ symbols \( \theta \in 2^P \) (i.e., \( \text{end} \neq \theta \), we set \( \delta(q_s, q_c, q_p, \theta) = (\delta_s(q_s, \theta), \delta_c(q_c, \theta), \delta_p(q_p, \theta)) \) where:

\[
\delta_s(q_s, \theta) = \begin{cases} 
q_{\text{bad}} & \text{if } q_s = q_{\text{bad}} \lor \delta(q_s, \theta) \in F_s \\
q_{\text{good}} & \text{otherwise}
\end{cases}
\]

\[
\delta_c(q_c, \theta) = \begin{cases} 
q_{\text{good}} & \text{if } q_c = q_{\text{good}} \lor \delta(q_c, \theta) \in F_c \\
q_{\text{bad}} & \text{otherwise}
\end{cases}
\]

For \( \theta \) with \( \text{end} \in \theta \), we set \( \delta(q_s, q_c, q_p, \theta) = q_T \) if \( \delta_s(q_s, \theta) \in F_s \) and \( \delta(q_c, q_p, \theta) = q_c \) in all other cases. Accepting state \( q_T \) is quasi-absorbing: \( \delta(q_T, \theta) = q_T \) when \( \text{end} \in \theta \), and \( \delta(q_T, \theta) = q_L \) otherwise. This forces winning

\[\text{if we want to have only a safe (resp. co-safe) constraint, it suffices to use a trivial constraint } \alpha_c = \top \text{ (resp. } \alpha_s = \bot (P 
\lor \neg P)).\]
strategies to output variable end at most once. Finally, \(q_1\) is an absorbing state: \(\delta(q_1, \theta) = q_1\) for every \(\theta \in 2^{P \cup \{\text{end}\}}\).

**Theorem 7.** The DBA \(\mathcal{A}_{\omega, \alpha}^{x} \) accepts infinite traces \(\pi\) such that either: (i) \(\pi(1) \cdots \pi(n) = \phi\) and end occurs only in \(\pi(n)\), or (ii) \(\pi \not\in A_1 \land A_2\), and end does not occur in \(\pi\). \(\mathcal{A}_{\omega, \alpha}^{x}\) can be constructed in double-exponential time in \(|A_1| + |A_2| + |\phi|\).

### 5.2 DBA Games

Once a specification has been converted into a DBA, realizability and synthesis can be reduced to DBA games. We briefly recall next the definition of how winning strategies can be computed.

A DBA (or Büchi) game (see e.g. (Chatterjee, Henzinger, and Piterman 2006)) is a two-player game given by a tuple \((X, Y, A)\), where \(X\) and \(Y\) are disjoint finite sets of variables and \(A\) is a DBA with alphabet \(2^{X \cup Y}\). A play is an infinite sequence of rounds, where in each round, Player I selects \(x_i \in X\), then Player II selects \(y_i \in Y\). A play is winning if it yields a word \((X_1 \cup Y_1)(X_2 \cup Y_2)\ldots \) that belongs to \(L(A)\).

A game is winning if there exists a strategy \(\sigma : (2^X)^* \rightarrow 2^Y\) such that for every infinite sequence \(X_1X_2\ldots \in X^\omega\), the word \((X_1 \cup y(X_1)) (X_2 \cup y(X_1X_2)) \ldots \) obtained by following \(\sigma\) belongs to \(L(A)\).

### 5.3 Constrained LTL\(_1\) Synthesis via DBA Games

Given a constrained LTL\(_1\) synthesis specification \((X, Y, \alpha, \varphi)\) with \(\alpha = A_1 \land A_2\), we proceed as follows:

1. Construct the DBA game \(G_{\alpha}^{x, \omega} = (X, Y \cup \{\text{end}\}, \mathcal{A}_{\omega, \alpha}^{x} \) .
2. Determine whether \(G_{\alpha}^{x, \omega}\) is winning; build \(Win(G_{\alpha}^{x, \omega})\) and check whether \((q_0, \alpha, \omega, q_0) \in Win(G_{\alpha}^{x, \omega})\).
3. If \(G_{\alpha}^{x, \omega}\) is not winning, return ‘unrealizable’.
4. Otherwise, compute a winning strategy for \(G_{\alpha}^{x, \omega}\) using the transducer from Section 5.2.

Using Theorems 7 and 8, we can show that this method is correct and yields optimal complexity:

**Theorem 9.** Consider a constrained LTL\(_1\) specification \(S = (X, Y, \alpha, \varphi)\) where \(\alpha\) (resp. \(\alpha\)) is a safe (resp. co-safe) formula. Then:

- \(S\) is realizable if the DBA game \(G_{\alpha, \omega}^{x, \omega}\) is winning;
- Every winning strategy for \(G_{\alpha}^{x, \omega}\) is a winning strategy for \(S\), and vice-versa;
- Deciding whether \(G_{\alpha}^{x, \omega}\) is winning, and constructing a winning strategy when one exists, can be done in \(2\text{EXP}\).

### 6 Synthesis of High-Quality Strategies

This section explores the use of a quantitative specification language to compare strategies based upon how well they satisfy the specification. We adopt the LTL\(_1\)[\(\mathcal{F}\)] language from (Almagor, Boker, and Kupferman 2016) and propose a new more refined way of defining optimal strategies.

#### 6.1 The Temporal Logic LTL\(_1\)[\(\mathcal{F}\)]

We recall here the language LTL\(_1\)[\(\mathcal{F}\)] proposed by Almagor, Boker, and Kupferman (2016). The basic idea is that instead of a formula being either totally satisfied or totally violated by a trace, a value between 0 and 1 will indicate its degree of satisfaction. In order to allow for different ways of aggregating formulae, the basic LTL syntax is augmented with a set \(\mathcal{F} \subseteq \{f : [0, 1]^k \rightarrow [0, 1] \mid k \in \mathbb{N}\}\) of functions, with the

\(^{3}\)Several \(Y\) may satisfy the conditions, and choosing any such \(Y\) yields a suitable transducer. Alternatively, one can use nondeterministic transducers (called strategy generators in (De Giacomo and Vardi 2015)) to encode a family of deterministic transducers.
choice of which functions to include in $T$ being determined by the application at hand.

Formally, the set of $\text{LTL}[T]$ formulae is obtained by adding $f(\varphi_1, \ldots, \varphi_n)$ to the grammar for $\varphi$, for every $f \in T$. We assign a satisfaction value to every $\text{LTL}[T]$ formula, finite trace $\pi$, and time step $1 \leq i \leq |\pi|$, as follows$^8$:

$$\llbracket \pi_i \rrbracket = 1 \quad \llbracket \pi, \bot \rrbracket = 0 \quad \llbracket \pi, \rho \rrbracket = \begin{cases} 1 \text{ if } p \in \llbracket \pi \rrbracket(i) \\ 0 \text{ otherwise} \end{cases}$$

$$\llbracket \pi, \neg \varphi \rrbracket = 1 - \llbracket \pi, \varphi \rrbracket$$

$$\llbracket \pi, \varphi_1 \land \varphi_2 \rrbracket = \min \{\llbracket \pi, \varphi_1 \rrbracket, \llbracket \pi, \varphi_2 \rrbracket\}$$

$$\llbracket \pi, f(\varphi_1, \ldots, \varphi_n) \rrbracket = f(\llbracket \pi, \varphi_1 \rrbracket, \ldots, \llbracket \pi, \varphi_n \rrbracket)$$

$$\llbracket \pi, \varphi_1 \cup \varphi_2 \rrbracket = \max \{\min \{\llbracket \pi, \varphi_1 \rrbracket, \min \{\llbracket \pi, \varphi_1 \rrbracket, \llbracket \pi, \varphi_2 \rrbracket\}\}$$

The (satisfaction) value of $\varphi$ on $\pi$, written $\llbracket \pi, \varphi \rrbracket$, is $\llbracket \pi, \varphi \rrbracket$.

We define $V(\varphi) \subseteq \{0, 1\}$ as the set of values $\llbracket \pi, \varphi \rrbracket$, ranging over all traces $\pi$ and steps $1 \leq i \leq |\pi|$. The following proposition, proven by (Almagor, Boker, and Kupferman 2016), shows that an $\text{LTL}[T]$ formula can take on only exponentially many different values.

**Proposition 1.** For every $\text{LTL}[T]$ formula $\varphi$, $V(\varphi) \leq 2^{|\varphi|}$.

The functions $f$ allow us to capture a diversity of methods for combining a set of potentially competing objectives (including classical preference aggregation methods like weighted sums and lexicographic ordering).

**Example 3.** For illustration purposes, consider two variants of our robot vacuum example, with specifications $\varphi_1$ and $\varphi_2$, in which the goal $\varphi_1(\text{clean}(LR) \land \text{clean}(BR))$ is replaced by $\varphi_1(\text{clean}(BR))$ and $\varphi_1(\text{clean}(LR))$, respectively. We can include in $T$ a binary weighted sum operator $\text{sum}_{0,0,0,0}$, where the satisfaction value of $\text{sum}_{0,0,0,0}(\varphi_1, \varphi_2)$ on trace $\pi$ is 0.3 if $\pi \models \varphi_1 \land \neg \varphi_2$, 0.7 if $\pi \models \neg \varphi_1 \land \varphi_2$, and zero otherwise. We can thus express that we’d like to clean both rooms, but give priority to the bedroom.

### 6.2 Defining Optimal Strategies

Henceforth, we consider a constrained synthesis $\text{LTL}[T]$ problem $(X, Y, \alpha, \varphi)$, defined as before except that now $\varphi$ is an $\text{LTL}[T]$ formula. Such formulae assign satisfaction values to traces, allowing us to rank traces according to the extent to which they satisfy the expressed preferences. It remains to lift this preference order to strategies.

Perhaps the most obvious way to rank strategies is to consider the minimum value of any trace induced by the strategy, preferring strategies that can guarantee the highest worst-case value. This is the approach adopted by (Almagor, Boker, and Kupferman 2016) for $\text{LTL}[T]$ synthesis. We formalize it for constrained $\text{LTL}[T]$ synthesis as follows:

**Definition 1.** The best guaranteed value of strategy $\sigma$, denoted $\text{bgv}(\sigma)$, is the minimum of $\llbracket \pi, \varphi \rrbracket$ over all $\pi \in \text{traces}(\sigma)$ (or 0 if $\text{traces}(\sigma) = \emptyset$). A strategy $\sigma$ is $\text{bgv}$-optimal w.r.t. $(\alpha, \varphi)$ if it is a $\alpha$-strategy and no $\alpha$-strategy $\sigma'$ exists with $\text{bgv}(\sigma') > \text{bgv}(\sigma)$.

Optimizing for the best guaranteed value seems natural, but can be insufficiently discriminative. Consider a simple scenario with $X = \{x\}$ and $Y = \{y\}$. If the environment plays $x$, then we get value 0 no matter what, and if $\neg x$ is played, a value of 1 is achieved by playing $y$, and 0 if $\neg y$ is played. Clearly, we should prefer to play $y$ after $\neg x$, yet the strategy that plays $\neg y$ following $\neg x$ is $\text{bgv}$-optimal, since like every strategy, its $\text{bgv}$ is 0. This motivates us to introduce a stronger, context-aware, notion of optimality:

**Definition 2.** Given a strategy $\sigma$, trace $\pi \in \text{traces}(\sigma)$ that does not contain end, and $X \in 2^X$, the best guaranteed value of $\sigma$ starting from $\pi, X$, written $\text{bgv}_{\pi,X}(\sigma)$, is the minimum of $\llbracket \pi, \varphi \rrbracket$ over all traces $\pi'$ in traces($\sigma$) such that $\pi \cdot (X \cup Y)$ for some $Y \in Y$ (or 0 if no such trace exists). A strategy $\sigma$ is strongly $\text{bgv}$-optimal w.r.t. $(\alpha, \varphi)$ if it is an $\alpha$-strategy, and there is no $\alpha$-strategy $\sigma'$, trace $\pi' \in \text{traces}(\sigma') \cap \text{traces}(\sigma')$ without end, and $X \in 2^X$ such that $\text{bgv}_{\pi,X}(\sigma') > \text{bgv}_{\pi,X}(\sigma)$.

Strongly $\text{bgv}$-optimal strategies take advantage of any favorable situation during execution to improve the best worst-case value. In the preceding example, they allow us to say that the first strategy is better than the second.

### 7 Algorithms: High-Quality $\text{LTL}[T]$ Synthesis

In this section, we present novel techniques to compute $\text{bgv}$-optimal and strongly $\text{bgv}$-optimal strategies for a constrained $\text{LTL}[T]$ synthesis problem $(X, Y, \alpha, \varphi)$. As in Section 5.1, we focus on the case where $\alpha$ is a conjunction $\alpha_1 \land \alpha_2$ of safe and co-safe formulae.

#### 7.1 Automaton for $\text{LTL}[T]$

It has been shown in (Almagor, Boker, and Kupferman 2016) how to construct, for a given $\text{LTL}[T]$ formula $\varphi$ and set of values $V \subseteq \{0, 1\}$, an NFA $\mathcal{A}_{\varphi,V} = (Q, \delta, \alpha, Q_0, F)$ that accepts finite traces $\pi$ with $\llbracket \pi, \varphi \rrbracket \in V$. We briefly recall the construction here. We denote by $\text{sub}(\varphi)$ the set of subformulas of $\varphi$, and let $C_{\varphi}$ be the set of functions $g : \text{sub}(\varphi) \rightarrow \{0, 1\}$ such that $g(\varphi) \in V(\varphi)$ for all $\psi \in \text{sub}(\varphi)$. $Q$ contains all consistent functions in $C_{\varphi}$, where a function $g$ is consistent if, for every $\psi \in \text{sub}(\varphi)$, the following hold:

- If $\psi = \top$, then $g(\psi) = 1$, and if $\psi = \bot$, then $g(\psi) = 0$.
- If $\psi \in \varphi$ then $g(\psi) \in \{0, 1\}$.
- If $\psi = f(\psi_1, \ldots, \psi_n)$, then $g(\psi) = f(g(\psi_1), \ldots, g(\psi_n))$.

The transition function $\delta$ is such that $g' \epsilon \delta(g, \psi)$ whenever $\sigma = \{p \in P \mid g(p) = 1\}$.

$\delta(g(\psi_1) \leq g(\psi_2))$ for every $\psi_1 \leq \psi_2$.

$g(\psi_1 \cup \psi_2) = \max \{g(\psi_1), g(\psi_2), g(\psi_1 \cup \psi_2))\}$ for every $\psi_1 \leq \psi_2$.

Finally, the set of initial states is $Q_0 = \{g \in Q \mid g(\varphi) \in V\}$, and $F = \{g \mid g(\varphi_1) \in \text{sub}(\varphi)\}$ for all $\psi_1, \psi_2 \in \text{sub}(\varphi)$ and $g[\varphi] = g(\varphi_1) \cup \{g \mid g(\varphi_1) = 0 \text{ for all } \psi_1 \in \text{sub}(g)\}$.

The NFA $\mathcal{A}_{\varphi,V}$ can be constructed in single-exponential time, and $L(\mathcal{A}_{\varphi,V}) = \{ \llbracket \pi, \varphi \rrbracket \in V\}$ (Almagor, Boker, and Kupferman 2016). By deterministic $\mathcal{A}_{\varphi,V}$, we obtain a DFA $\mathcal{A}_{\varphi,V}$ that accepts the same language and can be constructed in double-exponential time. In what follows, $V$ will always take the form $[b, 1]$, so we’ll use $\mathcal{A}_{\varphi,b}$ in place of $\mathcal{A}_{\varphi,[b,1]}$.
7.2 Synthesis of bgv-optimal strategies

We describe how to construct a bgv-optimal strategy. First note that given $b \in [0,1]$, we can construct a DBA $\mathcal{A}^b_{\text{DBA}}$ that recognizes traces such that either (i) $\alpha = \alpha_1 \land \alpha_2$ is violated and $\text{end}$ does not occur, or (ii) $\text{end}$ occurs exactly once and the induced finite trace $\pi$ is such that $[\pi, \varphi] \geq b$. Indeed, we simply reuse the construction from Section 5.1, replacing the DFA $\mathcal{A}_b$ with the DFA $\bar{\mathcal{A}}_{\text{DBA}}$. We next observe that an $\alpha$-strategy $\sigma$ with $\text{bgv}(\sigma) \geq b$ exists iff the DBA game $\langle X, Y, \emptyset \rangle$ is winning. Thus, by iterating over the values in $V(\varphi)$ in descending order, we can determine the maximal $b'$ for which an $\alpha$-strategy $\sigma$ with $\text{bgv}(\sigma) \geq b'$ exists. A bgv-optimal strategy can be computed by constructing a winning strategy for the DBA game $\langle X, Y, \emptyset \rangle$, using the approach in Section 5.2. As there are only exponentially many values in $V(\varphi)$ (Prop. 1), the overall construction takes double-exponential time.

Theorem 10. A bgv-optimal strategy can be constructed in double-exponential time.

7.3 Synthesis of strongly bgv-optimal strategies

To compute a strongly bgv-optimal strategy, we build a transducer that runs in parallel DBAs $\mathcal{A}^b_{\text{DBA}}$ for different values $b$, and selects outputs symbols so as to advance within the ‘best’ applicable winning region. This idea can be formalized as follows. As in Section 7.2, we first determine the maximal $b' \in V(\varphi)$ for which an $\alpha$-strategy $\sigma$ with $\text{bgv}(\sigma) \geq b'$ exists, and set $B = V(\varphi) \cap (b', 1]$. In the process, we will compute, for each $b \in B$, the sets $\text{Win}(G_b)$ and $\text{RA}(G_b)$ for the DBA game $G_b = \langle X, Y, B \rangle$ based on the DBA $\mathcal{A}^b_{\text{DBA}} = (\delta^b, \text{end}, Y^b, 0_b, 0_{\text{end}}, F_b)$. In the sequel, we will assume that the elements of $B$ are ordered as follows: $b_1 < b_2 \ldots < b_n$, with $b' = b_1$ and $b_0 = 1$.

We now proceed to the definition of the desired transducer $T_{\text{str}} = (2^X, 2^Y, \emptyset, Q_{\text{end}}, \delta_{\text{str}}, \omega_{\text{str}}, \omega_{\text{end}}, q_0^b)$, obtained by taking the cross product of the set of DBAs $\mathcal{A}^b_{\text{DBA}}$ with $b \in B$, in order to keep track of the current states in these automata:

- $q_0^b = (q_0^b, q_0^b, \ldots, q_0^b)$ and $Q_{\text{end}} = Q_{\text{end}} \times \ldots \times Q_{\text{end}}$,
- $\delta_{\text{str}}((q_1, \ldots, q_m), X) = (\delta_{\text{str}}(q_1, X \cup Y), \ldots, \delta_{\text{str}}(q_m, X \cup Y))$, where $Y = \omega_{\text{str}}(q_1, q_2, \ldots, q_m), X)$

After reading $X$, the output function identifies the maximal value $b \in B$ such that current state $q_0$ of $\mathcal{A}^b_{\text{DBA}}$ can transition, via some symbol $X \cup Y$, into a state in $\text{Win}(G_b)$, and it returns the same output as the transducer $T_{\text{str}}$ in state $q_0$:

- $\omega_{\text{str}}((q_1, \ldots, q_m), X) = \omega_{\text{str}}(q_0, X)$, where $b = \max\{|v| \in B \mid \exists Y \delta_{\text{str}}(q_1, X \cup Y) \in \text{Win}(G_b)\}$

We note that the transducer $T_{\text{str}}$ can be defined as in Section 5.2 even when $q_0^b \notin \text{Win}(G_b)$, but it only returns ‘sensible’ outputs when it transitions to $\text{Win}(G_b)$.

Theorem 11. $T_{\text{str}}$ implements a strongly bgv-optimal strategy and can be constructed in double-exponential time.

8 Discussion and Concluding Remarks

It has been widely remarked in the (infinite) LTL synthesis literature that environment assumptions are ubiquitous: the existence of winning strategies is almost always predicated on some kind of environment assumption. This was observed in the work of (Chatterjee, Henzinger, and Jobstmann 2008), motivating the introduction of the influential assume-guarantee synthesis model, and in work on rational synthesis (Fisman, Kupferman, and Lustig 2010), where the environment is assumed to act as a rational agent, and synthesis necessitates finding a Nash equilibrium. Interesting reflections on the role of assumptions in LTL synthesis, together with a survey of the relevant literature, can be found in (Bloom et al. 2014).

In this paper, we explored the issue of handling environment assumptions in LTL synthesis (De Giacomo and Vardi 2013), the counterpart of LTL synthesis for programs that terminate. Our starting point was the observation that the standard approach to handling assumptions in LTL synthesis (via logical implication) fails in the finite-trace setting. This led us to propose an extension of LTL synthesis that explicitly accounts for environment assumptions. The key insight underlying the new model of constrained LTL synthesis is that while the synthesized program must realize the objective in a finite number of steps, the environment continues to exist after the program terminates, so environment assumptions should be interpreted under infinite LTL semantics.

We studied the relationships holding between constrained LTL synthesis and (standard) LTL synthesis. In particular, we identified a fundamental difficulty in reducing constrained LTL synthesis to LTL synthesis – the former problem can require unbounded strategies, while bounded strategies suffice for the latter. Nevertheless, when the constraints were restricted to the safe LTL fragment, a reduction from constrained LTL synthesis to LTL synthesis is possible. Interestingly, this explains why planning – more naturally conceived as a constrained LTL synthesis problem – can also be encoded as LTL synthesis. The connection between synthesis and planning has been remarked in several works (see e.g., (De Giacomo and Vardi 2015; D’Ippolito, Rodríguez, and Sardiña 2018; Camacho et al. 2018a; 2018b; 2018c)). We also showed how to reduce constrained LTL synthesis to (infinite) LTL synthesis, which provides a worst-case optimal means of solving constrained LTL synthesis problems, in the general case, using (infinite) LTL synthesis tools. In the case where our constraint is comprised of a conjunction of safe and co-safe formulae, we showed that the constrained LTL synthesis problem can be reduced to DBA games and the winning strategy determined from the winning region. What makes our approach interesting is that the DBA is constructed via manipulation of DFAs, much easier to handle in practice than infinite-word automata.

We next turned our attention to the problem of augmenting constrained LTL synthesis with quality measures. We were motivated by practical concerns surrounding the ability to differentiate and synthesize high-quality strategies in settings where we may have a collection of mutually unrealizable objective formulae and alternative strategies of differing quality. Our work builds on results for the infinite case, e.g., (Almagor, Boker, and Kupferman 2016; Almagor et al. 2017; Kupferman 2016) with and without environment assumptions. We adopted LTL[$\mathcal{F}$] as our language for specifying quality measures. While the syntax of LTL[$\mathcal{F}$] is utilitarian, many more compelling preference
languages are reducible to this core language. We defined two different notions of optimal strategies – bgv-optimal and strongly bgv-optimal. The former adapts a similar definition in (Almagor, Boker, and Kupferman 2016) and the latter originates with us. We focused again on assumptions that can be expressed as conjunctions of safe and co-safe formulae and provided algorithms to compute bgv- and strongly bgv-optimal strategies with optimal (2EXP) complexity.

Proper handling of environment assumptions and quality measures, together with the design of efficient algorithms for such richer specifications, is essential to putting LTL synthesis into practice. The present paper makes several important advances in this direction and also suggests a number of interesting topics for future work including: the study of other types of assumptions in the finite-trace setting (e.g. rational synthesis), the exploitation of more compelling KR languages for specifying preferences, and the exploration of further ways of comparing and ranking strategies (perhaps incorporating notions of cost or trace length).

Relation to Conference Version

This paper appears in the Proceedings of the 16th International Conference on Knowledge Representation and Reasoning (KR 2018) without the appendix proofs. The body of this paper is the same as the KR 2018 paper, except that a minor typographic error in the translation of LTL into LTLf (the definition of τ(ϕ1 ∨ ϕ2) on page 6), which originally appeared in (De Giacomo and Vardi 2013) and was repeated in the KR 2018 paper, has been corrected.

Acknowledgements

This work was partially funded by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the ANR project GoAsQ (ANR-15-CE23-0022).

References


**Proofs**

**Theorem 5** The constrained LTL$_{μ}$ specification $S = \langle X, Y, α, ϕ \rangle$ is realizable iff the LTL$_{μ}$ specification $S^* = \langle X, Y, α', ϕ \rangle$ is realizable, where $α'$ is obtained from $α$ by replacing every occurrence of $ϕ$ by $¬ϕ$.

**Proof.** Let $σ'$ be a winning strategy for $S' = \langle X, Y, α' \rightarrow ϕ \rangle$, with $α$ a safe formula. We define a strategy $σ$ for $S = \langle X, Y, α, ϕ \rangle$ by setting $σ(X_1 \cdots X_n) = σ'(X_1 \cdots X_n)$ equal to

- $σ(X_1 \cdots X_n) \setminus \{\text{end}\}$, when $σ \in σ'(X_1 \cdots X_n)$ and $(X_1 \cup σ(X_1)) \cdots (X_n \cup σ(X_1 \cdots X_n)) \neq α'$;
- $σ(X_1 \cdots X_n \cup \{\text{end}\})$, otherwise.

To show that $σ$ is a winning strategy, take some $X \in (2^X)^ω$. Then $n_{σ,X} < ω$, and the finite trace $π' = π[σ',X]$ is such that (i) $π' \models ¬α'$, or (ii) $π' \models ϕ$ If (i) holds, then $n_{σ,X} = ω$ (since we will remove end), and $π = π[σ,X] \models ϕ$ is a prefix. We can then use the LTL$_{μ}$ equivalence $¬ϕ \equiv ω \rightarrow ϕ$ and the fact that $α$ is safe to derive $π \models ϕ$. If (ii) holds and (i) does not), then it follows from the definition of $σ$ that $n_{σ,X} = ω$ and $π = π[σ,X] = π[σ',X]$, so $π \models ϕ$.

For the other direction, let $σ$ be a winning strategy for $S$. Define a strategy $σ'$ for $S'$ by setting $σ'(X_1 \cdots X_n) = σ(X_1 \cdots X_n)$ equal to

- $σ(X_1 \cdots X_n) \cup \{\text{end}\}$, if $σ(X_1) \cdots (X_n \cup σ(X_1 \cdots X_n))$ is a bad prefix for $α$, and $σ' \not\in σ(X_1 \cdots X_n)$ for $k < n$;
- $σ(X_1 \cdots X_n) \cup \{\text{end}\}$, if $σ \in σ'(X_1 \cdots X_n)$ for some $k < n$;
- $σ(X_1 \cdots X_n) = σ(σ,X_1 \cdots X_n)$, otherwise.

Basically, $σ'$ mimics $σ$ and outputs end as soon as a bad prefix is reached or $σ$ terminates the execution due to satisfaction of $ϕ$, whichever situation occurs first. The construction of $σ'$ is such that executions always terminate which is not necessarily true for $σ$ – and induce finite traces that satisfy the LTL$_{μ}$ formula $α' \rightarrow ϕ$.

To show that $σ'$ is a winning strategy for $S'$, take some $X \in (2^X)^ω$. Consider the infinite induced trace $π = π[σ,X]$, and let $κ_X$ be the minimum $κ$ such that $π(1) \cdots π(κ)$ is a bad prefix for $α$. Since $κ_X < ω$, we examine these three cases separately: (i) $n_{σ,X} < ω$ and $κ_X \leq n_{σ,X}$, (ii) $n_{σ,X} < ω$ and $κ_X > n_{σ,X}$, and (iii) $n_{σ,X} = ω$. If (i) holds, then $n_{σ,X} = κ_X$ and $π' = π[σ',X] = π(1) \cdots π(κ_X)$ is a bad prefix for the safe formula $α$ and the LTL$_{μ}$ equivalence $¬ϕ \equiv ω \rightarrow ϕ$, we obtain $π' \models ϕ$.

If (ii) holds, then it follows from the definition of $σ'$ that $n_{σ,X} = κ_X$ and $π[σ',X] = π(1) \cdots π(n_{σ,X})$. Since $σ$ is a winning strategy for $S$ with $n_{σ,X} < ω$, we must have $π(1) \cdots π(n_{σ,X}) = ϕ$, hence $π[σ',X] = ϕ$.

If (iii) holds, then it must be the case that $π \models ϕ$ (because $ϕ$ is a safe formula). As $α$ is a safe formula, $π$ must contain a bad prefix for $α$, so $κ_X < ω$. Using a similar argument as in case (i), we can show that $π' \models ¬α'$.

**Theorem 7** The DBA $A_{μ,α}$ accepts infinite traces $π$ such that either: (i) $π(1) \cdots π(n) \models ϕ$ and end occurs only in $π(n)$,
or (ii) $\pi \not\vDash \alpha_1 \land \alpha_c$ and end does not occur in $\pi$. $\mathcal{A}_\phi^{p;\alpha}$ can be constructed in double-exponential time in $|\alpha_1| + |\alpha_c| + |\pi|$.

Proof. First, we prove that the language of $\mathcal{A}_\phi^{p;\alpha}$ contains the set of traces that satisfy one of the conditions (i) and (ii).

Then, we analyze the language of $\mathcal{A}_\phi^{p;\alpha}$ and demonstrate that the set of traces that satisfy one of the conditions (i) and (ii).

The construction of $\mathcal{A}_\phi^{p;\alpha}$ is polynomial in the size of $\mathcal{A}_\phi$, $\mathcal{A}_\phi$, and $\mathcal{A}_\phi$, which can be constructed in double-exponential time in $|\alpha_1| + |\alpha_c| + |\pi|$, respectively.

(2) (i) If $\pi(1) \cdots \pi(n) \models \phi$ and end occurs only in $\pi(n)$, then the run of $\mathcal{A}_\phi$ on $\pi(1) \cdots \pi(n)$ is accepting, i.e., its last state belongs to $F$. Then it follows from the definition of $\mathcal{A}_\phi^{p;\alpha}$ that the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ will transition to $q_\pi$ after reading $\pi(n)$ and, because end occurs only in $\pi(n)$, it will then loop at $q_\pi$. Since $q_\pi$ is an accepting state of $\mathcal{A}_\phi^{p;\alpha}$, this shows that $\mathcal{A}_\phi^{p;\alpha}$ accepts $\pi$. (ii) If $\pi \not\vDash \alpha_1 \land \alpha_c$ and end does not occur in $\pi$, then either $\pi \not\vDash \alpha_1$ or $\pi_\not\vDash \alpha_c$. In the first case ($\pi \not\vDash \alpha_1$), the trace $\pi$ contains a bad prefix $\pi(1) \cdots \pi(n)$, and w.l.o.g. we can suppose that this is the shortest such prefix. Then it follows that the run of $\mathcal{A}_\phi$ on $\pi(1) \cdots \pi(n)$ is accepting. From the definition of $\mathcal{A}_\phi^{p;\alpha}$, the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ transitions to a state $(q_\pi, q_\alpha, q_\phi)$ where $q_\pi = q_{bad}$. Because end does not occur in $\pi$, after having read $\pi(n)$, the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ will remain among the states whose third component is $q_{bad}$. By construction, these states are accepting, so $\mathcal{A}_\phi^{p;\alpha}$ accepts $\pi$. In the second case ($\pi \not\vDash \alpha_c$), the run of $\mathcal{A}_\phi$ on finite prefix $\pi(1) \cdots \pi(n)$ is not accepting for any $n < \infty$. It follows that the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ will not visit any state $(q_\pi, q_\alpha, q_\phi)$ with $q_\pi = q_{good}$, and since $\pi$ does not contain end, it also cannot contain the state $q_{good}$. Thus, the run of $\pi$ will only visit accepting states. Then, $\mathcal{A}_\phi^{p;\alpha}$ accepts $\pi$.

(3) Let $\pi$ be an infinite trace that is accepted by $\mathcal{A}_\phi^{p;\alpha}$. We distinguish three cases: (a) end does not occur in $\pi$; (b) end occurs exactly one time in $\pi$; (c) end occurs more than one time in $\pi$. Case (a): if end does not occur in $\pi$, then $q_{\pi}$ does not occur in the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$. As this run is accepting but does not contain $q_{\pi}$, it must either hit infinitely often states with $q_{bad}$, or hit infinitely often states without $q_{good}$. In the first case, let $\pi(1) \cdots \pi(n)$ be the smallest prefix of $\pi$ such that after reading $\pi(1) \cdots \pi(n)$, the DBA $\mathcal{A}_\phi^{p;\alpha}$ enters a state $(q_\pi, q_\alpha, q_\phi)$ with $q_\pi = q_{bad}$. By construction of $\mathcal{A}_\phi^{p;\alpha}$, it must be the case that $\mathcal{A}_\phi$ on $\pi(1) \cdots \pi(n)$ is accepting. Thus, $\pi(1) \cdots \pi(n)$ is a bad prefix of $\alpha_c$, which means $\pi \not\vDash \alpha_c$. In the second case, we observe that if a run enters a state $(q_\pi, q_\alpha, q_\phi)$ with $q_\pi = q_{good}$, then it remains in a state with $q_{good}$ in the second component unless a symbol with end is read. As the considered trace $\pi$ does not contain end, it follows that the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ does not hit any state $(q_\pi, q_\alpha, q_\phi)$ with $q_\pi = q_{good}$. Hence, $\mathcal{A}_\phi$ must not accept any finite prefix of $\pi$, nor $\pi$ does not contain any good prefixes for $\alpha_c$, i.e., $\pi \not\vDash \alpha_c$. This concludes that case (a) implies case (i). Case (b): suppose that end occurs exactly one time in $\pi$, say in the $n$th symbol $\pi(n)$. Immediately after reading $\pi(n)$, the DBA $\mathcal{A}_\phi^{p;\alpha}$ will transition to either $q_{\pi}$ or $q_{l}$. However, since the run of $\mathcal{A}_\phi^{p;\alpha}$ on $\pi$ is accepting, it cannot contain $q_{l}$. We thus have a transition of the form $\delta(q_\pi, q_\alpha, q_\phi, \pi(n)) = q_{\pi}$ with $\delta(q_{\pi}, \pi(n)) \in F_{\phi}$. It follows that the finite prefix $\pi(1) \cdots \pi(n)$ is accepted by the DBA $\mathcal{A}_\phi$.

Theorem 9 Consider a constrained LTL₁ specification $S = (X, Y, \alpha_1 \land \alpha_c, \varphi)$ where $\alpha_1$ (resp. $\alpha_c$) is a safe (resp. co-safe) formula. Then:

- $S$ is realizable iff the DBA game $G_{\pi,c}^{p;\alpha}$ is winning;
- Every winning strategy for $G_{\pi,c}^{p;\alpha}$ is a winning strategy for $S$, and vice-versa;
- Deciding whether $G_{\pi,c}^{p;\alpha}$ is winning, and constructing a winning strategy when one exists, can be done in 2EXP.

Proof. By Theorem 7, the language of the DBA $\mathcal{A}_\phi^{p;\alpha}$ contains all, and only, the infinite traces $\pi$ such that either: (i) $\pi(1) \cdots \pi(n) \models \varphi$ and end occurs only in $\pi(n)$, or (ii) $\pi \not\vDash \alpha_1 \land \alpha_c$ and end does not occur in $\pi$. By definition, a strategy $\sigma$ is a winning strategy for $G_{\pi,c}^{p;\alpha}$ iff every induced infinite trace $\pi[\sigma, X]$ is accepted by $\mathcal{A}_\phi^{p;\alpha}$. It follows that winning strategies for $G_{\pi,c}^{p;\alpha}$ are winning strategies for $S$, and vice versa. By Theorem 7, we can construct the DBA $\mathcal{A}_\phi^{p;\alpha}$ in double-exponential time. We can then construct, in polynomial time in $|\mathcal{A}_\phi^{p;\alpha}|$, the set $\text{Win}(G_{\pi,c}^{p;\alpha})$ and check whether $(q_{\pi_0}, q_{\pi_1}, q_{\pi_2}) \in \text{Win}(G_{\pi,c}^{p;\alpha})$. If the latter holds, then we construct a winning strategy in the form of a transducer. This step is also polynomial w.r.t. $|\mathcal{A}_\phi^{p;\alpha}|$, and thus the entire procedure can be performed in double-exponential time.

Theorem 10 A bgv-optimal strategy can be constructed in double-exponential time.

Proof. We first argue that the described construction yields an bgv-optimal strategy. We know from (Almagor, Boker, and Kupferman 2016) that the $\mathcal{A}_\phi^{p;\alpha}$ accepts finite traces $\pi$ such that $[\pi, \varphi] \geq b$. By reusing the arguments from the proof of Theorem 7, we can show that $\mathcal{A}_\phi^{p;\alpha}$ recognizes infinite traces such that either (i) $\alpha = \alpha_1 \land \alpha_c$ is violated and end does not occur, or (ii) end occurs exactly once and the induced finite trace $\pi$ is such that $[\pi, \varphi] \geq b$. It follows that an $\alpha$-strategy $\sigma$ with $bvg(\sigma) \geq b$ exists if the DBA game $\langle X, Y \cup \{\text{end}\}, \mathcal{A}_\phi^{p;\alpha} \rangle$ is winning. We can use the techniques described in Section 5.2 to decide whether such a DBA is winning. By considering the values in $V(\varphi)$ in descending order, we can determine the maximal $b'$ for which an $\alpha$-strategy $\sigma$ with $bvg(\sigma) \geq b'$ exists. We can then compute such a strategy, for the identified best value $b'$, by constructing a winning strategy for the DBA game $\langle X, Y \cup \{\text{end}\}, \mathcal{A}_\phi^{p;\alpha} \rangle$, again using the techniques from Section 5.2.
time. It follows that $\mathcal{A}_{\omega}^{\pi}$ can also be constructed in double-exponential time. Determining whether the DBA game $(X, \mathcal{Y} \cup \{\text{end}\}, \mathcal{A}_{\omega}^{\pi})$ is winning, and constructing a winning strategy for the game, is also in double-exponential time. Finally, we note that all of the preceding double-exponential time operations are performed at most once per value $b \in V(\varphi)$, so the overall procedure runs in double-exponential time.

The next two lemmas will be used to prove Theorem 11. In what follows, it will be convenient to slightly abuse notation and use $\delta(q, \pi)$, with $\pi$ a finite trace, to indicate the automata state resulting from reading $\pi$ starting from state $q$ (and similarly for the output function $\omega$ of transducers on a finite string $X_1 \ldots X_n$).

**Lemma 1**. For every $\pi = (X_1 \cup 1) \ldots (X_n \cup Y_n) \in 2^{X_n \cup Y_n}$, $X_{n+1} \in 2^X$, and $b \in [0, 1]$, the following are equivalent:

1. there exists an $\alpha$-strategy $\sigma$ such that $\pi \in \text{ptraces} (\sigma)$ and $b_{\text{g.v.m}}_{\alpha}(\pi) \geq b$,

2. $\delta_b(q_{q_0}^\pi, \pi(\{X_1 \cup 1\} \cup \{X_n \cup Y_n\})) \in \text{Win}(G_\text{b})$ for some $Y_{n+1} \in 2^{Y_n \cup \{\text{end}\}}$.

**Proof.** $(\Rightarrow)$ Suppose that $\sigma$ is an $\alpha$-strategy such that $\pi \in \text{ptraces} (\sigma)$ and $b_{\text{g.v.m}}_{\alpha}(\pi) \geq b$. Set $Y_{n+1} = \sigma(X_1 \ldots X_n \cup 1)$, and let $q' = \delta_b(q_{q_0}^\pi, \pi(\{X_1 \cup 1\} \cup \{X_n \cup Y_n\}))$. Consider the DBA $\mathcal{A}_{\omega}^{q'}$ = $(2^{(X_n \cup \{\text{end}\})}, Q_0, \delta_b, q', F_b)$, which is the same as $\mathcal{A}_{\omega}^{q_0}$ but with $q'$ for the initial state. Define a strategy $\sigma'$ for the DBA game $G_{\text{b}} = (X, \mathcal{Y} \cup \{\text{end}\}, \mathcal{A}_{\omega}^{q_0})$ as follows:

$$
\sigma'(X_1 \ldots X_n) = \sigma(X_1 \ldots X_n \cup 1 \ldots X')
$$

We claim that $\sigma'$ is a winning strategy for $G_{\text{b}}$. To see why, take any $X \in (2^X)^*$, and let $\pi_X^\sigma = [\pi(\sigma, X)]$. We need to show that $\pi_X^\sigma$ is accepted by $\mathcal{A}_{\omega}^{q_0}$. Let us consider $\pi_X = \pi[\sigma(X_1 \ldots X_n, X)]$, and let $s_0 \ldots s_j \ldots$ be the infinite run of $\mathcal{A}_{\omega}^{q_0}$ on $\pi_X$. Note that since $\pi \in \text{ptraces}(\sigma)$, we know that $\pi \subseteq \pi_X$, hence either (i) $\pi_X$ does not contain end and $\pi \in \pi' \alpha$, or (ii) $\pi_X$ contains exactly one occurrence of end (at some position $k \leq n + 1$, since $\pi$ does not contain end) and the induced finite trace $\pi_X'$ is $\pi'[\sigma, X_1 \ldots X_n, X] = \pi'$ is such that $[\pi_X', \varphi] \geq b$. It follows that $\pi_X$ is accepted by $\mathcal{A}_{\omega}^{q_0}$, and thus the infinite run $s_0 \ldots s_j \ldots$ of $\mathcal{A}_{\omega}^{q_0}$ on $\pi_X$ contains infinitely many $s_j \in F_b$. We then observe that $s_{n+1} = q'$. Since $\mathcal{A}_{\omega}^{q_0}$ has the same transitions as $\mathcal{A}_{\omega}^{q_0}$, it follows that $s_{n+1} s_{n+2} \ldots$ is the run of $\mathcal{A}_{\omega}^{q_0}$ on $\pi_X$. Note that $s_{n+1} s_{n+2} \ldots$ must also contain infinitely many $s_j \in F_b$, so it is an accepting run. We have thus shown that $\sigma'$ is a winning strategy for $G_{\text{b}}$.

As the game $G_{\text{b}}$ is winning, we must have $q' \in \text{Win}(G_{\text{b}})$. We then remark that since $G_{\text{b}}$ and $G_{\text{b}}$ only differ in their initial states, the two games have precisely the same winning regions. We thus obtain $\pi' = \delta_b(q_{q_0}^\pi, \pi(\{X_1 \cup \{1\} \cup \{X_n \cup Y_n\})) \in \text{Win}(G_{\text{b}})$.

$(\Leftarrow)$ Suppose that $\pi' = \delta_b(q_{q_0}^\pi, \pi(\{X_1 \cup \{1\} \cup \{X_n \cup Y_n\})) \in \text{Win}(G_{\text{b}})$. By following the strategy of the transducer $T_{\text{b}}$, from this point on, we are guaranteed to produce a trace that is accepted by the automaton $\mathcal{A}_{\omega}^{q_0}$. More precisely, consider the strategy $\sigma$ defined as follows:

- $\sigma(X_1 \ldots X_n) = Y_k$, if $X_1 \ldots X_n = X_1 \ldots X_k$ (1 ≤ k ≤ n + 1)
- $\sigma(X_1 \ldots X_n) = \omega_b(q_{b_{\text{g.v.m}}}(q', X_1 \ldots X_n), X_{n+1})$, if $X_1 \ldots X_n = X_1 \ldots X_k \land X_{n+1} = \pi(X_1 \ldots X_n) \in \pi'$ and $\pi'$ contains a single occurrence of end.

We claim that $\sigma$ is an $\alpha$-strategy such that $(X_1 \cup 1) \ldots (X_n \cup Y_n) \in \text{ptraces}(\sigma)$ and $b_{\text{g.v.m}}_{\alpha}(\pi) \geq b$. As noted above, the first bullet of the definition ensures that $(X_1 \cup 1) \ldots (X_n \cup Y_n) \in \text{ptraces}(\sigma)$. The last three bullets make sure that every $\pi' \in \text{traces}(\sigma)$ with $(X_1 \cup 1) \ldots (X_n \cup Y_n) \in \pi'$ contains exactly one occurrence of end. It remains to consider the infinite traces that begin with $(X_1 \cup 1) \ldots (X_n \cup Y_n)$. Consider some such trace $\pi' = (X_1 \cup 1) \ldots (X_2 \cup Y_2) \ldots$ in traces(\sigma), and let $s_0 s_1 s_2 \ldots$ be the infinite run of $\mathcal{A}_{\omega}^{q_0}$ on $\pi'$. Because $(X_1 \cup 1) \ldots (X_n \cup Y_n) \subseteq \pi'$, we know that $s_{n+1} = q'$. The latter can be combined with the second bullet to show that for every $i \geq n + 1$, $Y_i = \omega_b(q_{b_{\text{g.v.m}}}(q', X_{n+1}), s_{n+1}) = \delta_b(s_{n+1}, X_{n+1})$. As $s_{n+1} = q' \in \text{Win}(G_{\text{b}})$, and $\omega_b$ is defined so as to always remain within $\text{Win}(G_{\text{b}})$, we have $s_i \in \text{Win}(G_{\text{b}})$ for every $i \geq n + 1$. Furthermore, since $\omega_b$ always reduces the distance to $\text{RA}(G)$, there are infinitely many $i \geq n + 1$ such that $s_i \in F_b$. This establishes that $s_0 s_1 s_2 \ldots$ is an accepting run, and thus, $\pi'$ must either be such that $\pi' \in \pi'$, or it contains a single occurrence of end such that the infinite induced trace $\pi''$ is such that $[\pi'', \varphi] \geq b$. We have thus shown that every infinite trace produced by $\sigma$ either violates $\alpha$ or contains end, i.e. $\sigma$ is an $\alpha$-strategy. Moreover, for every $\pi'' \in \text{traces}(\sigma)$ with $(X_1 \cup 1) \ldots (X_n \cup Y_n) \subseteq \pi''$, we have $[\pi'', \varphi] \geq b$, as desired.

In the following lemma, we use $\sigma_{\text{gr}}$ to denote the strategy implemented by the transducer $T^\varphi$. To simplify the formulation, we extend the notation $b_{\text{g.v.m}}(\pi)$ to all finite traces that can be produced by strategy $\sigma$ (recall that Definition 2 only defines this notation for compatible traces that do not contain end). Formally, given a trace $\pi = (X_1 \cup 1) \ldots (X_n \cup Y_n)$ that is a prefix of some infinite trace in $\pi[\sigma, X]$ and contains end at position $k \leq n$, we set $b_{\text{g.v.m}}(\pi) = [\pi', \varphi]$, where $\pi' = (X_1 \cup 1) \ldots (X_k \cup Y_k \cup \{\text{end}\})$.

**Lemma 2.** For every $X_1, \ldots, X_n \in (2^X)^*$, $X_{n+1} \subseteq X$, and $v \in [0, 1]$, if $\pi = (X_1 \cup \omega_b(q_{q_0}^\pi, X_1), \ldots, X_n \cup \omega_b(q_{q_0}^\pi, X_1, \ldots, X_n))$, $(q_1, q_2, \ldots, q_m) = \delta_b(q_{q_0}^\pi, X_1, \ldots, X_n)$, and $u$ is such that
\(\omega_{\text{bgv}}((q_1, q_2, \ldots, q_m), X_{n+1})\) was set equal to \(\omega_b(q_n, X_{n+1})\), then \(\text{bgv}_{x_n,\pi}(\sigma_{\text{str}}) \geq u\).

**Proof.** Fix \(X_1, \ldots, X_n \in (2^X)^r\) and \(X_{n+1} \subseteq X\). Consider some \(X \in (2^X)^r\) such that \(X = X_1 \cup \cdots \cup X_n \cup X_{n+2} \cup \cdots\). Let \(\pi' = \pi|_{[r_{\text{bgv}}]}\) be the unique value \(b\) in \([b_1, \ldots, b_m]\) such that \(\omega_{\text{bgv}}((q_1', q_2', \ldots, q_m'), X_1 \cup \cdots \cup X_n)\) was set equal to \(\omega_b(q_n', X_{n+1})\). Basically, \(\pi' = b\) means that we used transducer \(G_b\) to generate \(Y_{n+1}\) after reading \(X_{n+1}\) from state \((q_1', q_2', \ldots, q_m')\). Note that the value \(u\) from the lemma statement is equal to \(\zeta(n)\).

**Claim:** For all \(i \geq 0\), \(\zeta(i + 1) \geq \zeta(i)\).

**Proof of claim:** Suppose that \(\zeta(i) = b\), which means that \(b = \max\{v \in B \mid \exists Y \delta_i(q_i', X_1 \cup Y) \in \text{Win}(G_i)\}\). Then we have \(Y_{n+1} = \omega_b(q_n', X_{n+1})\). From the definition of \(\omega_b\), and the fact that there exists some \(Y\) with \(\delta_i(q_i', X_1 \cup Y) \in \text{Win}(G_i)\), we know that \(\delta_i(q_i', X_1 \cup Y) \in \text{Win}(G_b)\). It follows that there exists \(Y'\) such that \(\delta_i(q_i', X_1 \cup Y') \in \text{Win}(G_b)\), and hence \(\max\{v \in B \mid \exists Y' \delta_i(q_i', X_1 \cup Y') \in \text{Win}(G_i)\} \geq b\). Thus, \(\zeta(i + 1) \geq \zeta(i)\) and \(\zeta(i) \leq \zeta(h)\) for \(i < h\). Let \(b_X = \zeta(h)\). Observe that \(q_0, q_1, q_2, \ldots\) is the run of \(\mathcal{R}_{\text{bgv}}^\pi\) on \(\pi'\), and \(q_0, q_1, q_2, \ldots \in \text{Win}(G_b)\). From the definition of \(\omega_{\text{bgv}}\), we can infer that \(q_i, q_i, q_i, \ldots \in \text{Win}(G_{\pi'})\) for all \(i \geq h\), and further that there are infinitely many \(q_i, q_i, q_i, \ldots \in \text{Win}(G_{\pi'})\). This means that \(b_X = \zeta(h) \geq \zeta(n)\). We have shown that every trace \(\pi'\) in \(\text{traces}(\sigma_{\text{str}})\) of \(\sigma_{\text{str}}\) is such that \(\|\pi', \varphi\| \geq \zeta(n) = u\), and hence that \(\text{bgv}_{x_n,\pi'}(\sigma_{\text{str}}) \geq u\).

We now proceed to the proof of Theorem 11.

**Theorem 11** 
\(\mathcal{T}_{\text{str}}\) implements a strongly bgv-optimal strategy and can be constructed in double-exponential time.

**Proof.** We first show that \(\mathcal{T}_{\text{str}}\) implements a strongly bgv-optimal strategy. Suppose for a contradiction that this is not the case. Then there exists a finite trace \(\pi = (X_1 \cup Y_1) \cup \cdots \cup (X_n \cup Y_n) \in \text{ptraces}(\sigma)\) that does not contain \(\text{end}\), \(X \in X\), and an \(\alpha\)-strategy such that \(\pi \in \text{ptraces}(\sigma')\) and \(\text{bgv}_{x,\pi}(\sigma') > \text{bgv}_{x,\pi}(\sigma)\). Suppose that \(\text{bgv}_{x,\pi}(\sigma) = b\) and \(\text{bgv}_{x,\pi}(\sigma') = b'\). From Lemma 1, we know that \(\delta_{v}(q_0', \pi(X_1 \cup Y_1)) \in \text{Win}(G_b)\) for some \(Y_1 \in 2^Y(\text{end})\). It follows that \(\omega_{\text{bgv}}(\delta_{v}(q_0', X_1 \cup Y_1), X_{n+1}) = \omega_{b}(q_i, X_{n+1})\) for some \(v \geq b'\). From Lemma 2, \(\text{bgv}_{x,\pi'}(\sigma_{\text{str}}) \geq v \geq b'\), a contradiction.

We know from Section 7.2 and Theorem 10 that for each \(v \in V(\varphi)\), the DBA \(\mathcal{A}_{\text{bgv}}^\pi\) winning region \(\text{Win}(G_b)\), and transducer \(G_b\) can be constructed in double-exponential time. As there are only single exponentially many values in \(V\) (hence \(B\)), the transducer \(\mathcal{T}_{\text{str}}\) can also be constructed double-exponential time.